CHAPTER 5

INSTALLATION ACCESS AND CIRCULATION CONTROL

0500. GENERAL

a. A system of personnel and vehicle movement control is a required basic security measure at Navy installations and activities. The degree of control must be in keeping with the sensitivity, classification, value or operational importance of the area. Visitor control relative to classified information will be in compliance with reference (a). Procedures will be coordinated among activities in the same geographical region when appropriate and feasible.

b. This chapter prescribes general policies for controlling entry into and exit from Navy installations. Access control is an integral part of the installation physical security program. Each installation or separate activity commanding officer must clearly define the access control measures (tailored to local conditions, e.g., Navy training "campuses") required to safeguard facilities and ensure accomplishment of the mission.

c. This chapter also prescribes policies for establishment of restricted areas whether by host installations, tenant activities, or by separate activities.

0501. POLICY. It is DoD policy that procedures to control access to installations and separate activities shall be developed, established, and maintained, including the following:

a. Using a defense-in-depth concept to provide gradated levels of protection from installation perimeter to critical assets.

b. Establish positive access control measures at entry control points to installations.

c. Determining the degree of control required over personnel and equipment entering or leaving the installation.

d. Prescribing procedures for inspecting persons, their property and vehicles at entry and exit points of installations or at designated secure areas within an installation, and while on the installation.

(1) This shall include determination of whether inspections are randomly conducted or mandatory for all.

(2) All procedures shall be reviewed for legal sufficiency by the appropriate general counsel or legal advisor to the Navy installation/activity prior to issuance.

e. Enforcing the removal of, or denying access to, persons who are a threat to order, security, and the discipline of the installation.

f. Designating restricted areas to safeguard property or material for which the commander is responsible.

g. Using randomized antiterrorism measures within existing security operations to reduce patterns, change schedules and visibly enhance the security profile of an installation. This reduces the effectiveness of preoperational surveillance by hostile elements.

0502. INSTALLATION ACCESS. Installation/activity commanding officers shall:

a. In addition to required armed guards, determine additional security controls of perimeter gates, i.e., barriers, video surveillance, explosives detection, vehicle inspection capabilities, etc. This determination should be based upon the results of the review and assessment processes discussed in chapter 1 and considerations discussed in chapter 2 of this manual.

b. Allocate resources necessary to enforce the established controls. These controls will be monitored and evaluated to ensure adequate protection is maintained.

0503. ACCESS AUTHORIZATION AND CONTROL SYSTEM REQUIREMENT

a. The methods used to control personnel access at an activity will be included in written procedures in the Physical Security Plan, and will include the following:

(1) Designation of restricted areas.

(2) Description of access control methods in use.

(3) Method for establishing authorization for entering and leaving each area, as they apply to both personnel continually authorized access to the area and to visitors, including any special provisions concerning non-duty hours.

(4) Details of where, when, and how security badges will be displayed.

(5) Procedures to be followed in case of loss or damage to security badges.

(6) Procedures to recover issued security badges.

(7) Measures to deny illicit use of lost, stolen, sold, or other illegally acquired security badges.

0504. EMERGENCY PLANNING

a. Installation/activity commanding officers will plan for increasing vigilance and restricting access at installations/activities under the following situations:

(1) National emergency.

(2) Disaster.

(3) Terrorist threat conditions (see references (g) through (j) for further information).

(4) Significant criminal activity.

(5) Civil disturbance.

(6) Other contingencies that would seriously affect the ability of installation personnel to perform their mission.

b. Planning should include the following:

(1) Coordination with local, State, Federal, or host country officials to ensure integrity of restricted access to the installation and reduce the effect on surrounding civilian communities;

(2) Establishment of a system for positive identification of personnel and equipment authorized to enter and exit the installation;

(3) Maintenance of adequate physical barriers that will be installed to control access to the installation;

(4) Predesignation of posts to be manned, personnel, equipment, and other resources to enforce restricted access and respond to incidents;

(5) Exercising contingency plans to validate their effectiveness, including systems for alerting and evacuation of personnel.

0505. AREA PROTECTION AND CONTROL

a. Prior to making decisions to employ additional physical security measures for a specific area(s) within the installation or activity, a thorough risk and threat analysis must be performed to determine the degree of physical security required.

(1) The continuing review and assessment processes described earlier in chapter 1, and the planning considerations outlined in chapter 2 are to be used.

(2) Only after these factors are addressed can appropriate controls for specific areas be decided on and instituted.

b. Restricted Areas

(1) Restricted areas are designated in writing by a commanding officer who has jurisdiction over the area. These areas are established under DoD Directive 5200.8 of 25 April 1991 (enclosed in reference (s)), and Section 21, Internal Security Act of 1950; Ch. 1024, 64 stat. 1005; 50 U.S.C. 797).

(2) General policies and standards for restricted areas are outlined in appendix VI.

c. Enclave Security Concept. Essentially, enclaving is the provision of concentrated security measures at specific sites, usually designated as restricted areas, within an installation or activity, such as flightline areas and waterside areas or other large critical/essential assets for which a higher degree of protection is appropriate.

0506. WATER BOUNDARIES. Water boundaries present special security problems. Such areas should be protected by barriers, and posted. In addition to barriers, patrol craft should be used at activities or installations whose waterfronts contain critical assets, or which are otherwise essential to the mission of the installation or activity. In inclement weather, such patrols cannot provide an adequate degree of protection, and should be supplemented by increased waterfront patrols, watch towers, military working dog teams, and other appropriate waterside security systems.

0507. ENFORCEMENT OF MOVEMENT CONTROL

a. Enforcement of movement control systems for restricted areas rests primarily with the activity personnel who normally work in the areas.

(1) If this control is based on personal recognition, all personnel in restricted areas will be instructed to consider each unrecognized individual as a person whose authorization to be in the area is in doubt, and to maintain observation of and report them to their supervisor, the security officer, or other appropriate authority.

(2) If security badges are used, all personnel will be similarly instructed to consider each unbadged or an apparently improperly security badged individual as a person whose authorization to be in the area is in doubt, and to similarly report their presence.

b. Written procedures will be incorporated into the local Physical Security Plan to cover these requirements.

c. Consideration may be given to the use of CNO-approved, commercially available access control systems to enhance enforcement of movement controls within a facility. These

systems facilitate access control, while reducing the number of personnel required.

0508. SIGNS AND POSTING OF BOUNDARIES. Signs and posting of boundaries are addressed in appendix VII.

0509. VEHICLE MOVEMENT CONTROL. Vehicles will be controlled as necessary to:

a. Control movement of the personnel associated with the vehicles.

b. To manage risk of using vehicles for unauthorized removal of government property or bringing aboard unauthorized items.

c. To manage risk of vehicle bombs. To mitigate the effectiveness of a vehicle bomb attack, commanders shall be continually vigilant against allowing vehicle parking near high-density, soft target buildings. Every attempt should be made to establish a minimum of a 50-foot stand-off where possible. Parking regulations should be strictly enforced. During THREATCON Bravo, commanders will achieve a 100-foot or more vehicle stand-off from high density soft targets. AT THREATCON Charlie or Delta, a 400-foot stand-off should be achieved. Centralized or remote parking should be instituted at THREATCON Charlie or higher. Traffic patterns shall be a consideration in AT/FP plans.

0510. PARKING OF PRIVATELY OWNED VEHICLES

a. Privately owned vehicles should not be parked in any restricted area, as such parking exacerbates the risks and increases resources required to maintain appropriate access control.

b. Privately owned vehicles should not be parked near doorways leading into or from buildings primarily used for the manufacture, repair, rework, storage, handling, packaging or shipping of government material and supplies.

c. Parking decisions should also consider means of minimizing danger in the event of vehicular fire or explosion.

0511. ADMINISTRATIVE INSPECTION OF VEHICLES

a. All vehicles on Navy installations are to be subject to administrative inspection according to procedures authorized by the commanding officer. As ordered and directed by the commanding officer, authorized security personnel will administratively inspect vehicles entering or leaving the installation. Such inspections are deemed reasonably necessary to protect the premises, material and utilities from loss, damage or destruction.

b. To be effective, these administrative inspections must be conducted frequently enough so that personnel remain mindful that the inspections are a real possibility, and that they could be inspected at any time they enter or leave the area.

c. It is better to frequently conduct inspections of a few vehicles at any one time than to infrequently inspect a lot of vehicles at any one time.

d. No person or group may be exempted from, or singled out for, such inspections, and the instruction by commanding officers regarding such inspections shall be coordinated in advance of implementation with local Judge Advocate General (JAG) or Naval Legal Service Office officials to ensure strict adherence to either mandatory inspection of all vehicles or a structured random inspection pattern that is impartial and unbiased.

e. Naval Criminal Investigative Service. Naval Criminal Investigative Service (NAVCRIMINVSERV) personnel, upon presentation of their special agent credentials when entering or leaving Navy installations, vehicles used by them in the course of official business, and all occupants therein are exempt from administrative inspections, per reference (t).

0512. SPECIAL PRECAUTIONS. Personnel responsible for the accomplishment or implementation of personnel and vehicle control procedures shall at all times be watchful for the unauthorized introduction to or removal from the installation of government property, especially weapons, ammunition and explosive materials. This includes all personnel and means of transportation, including government, private and commercial vehicles, aircraft, railcars, and ships.

0513. CONTROL AND ACCOUNTABILITY OF PERSONAL WEAPONS

a. All personal weapons brought aboard a Navy installation or activity must be registered with the security department. Weapons which must be registered shall include:

(1) Pistols/revolvers.

(2) Crossbows.

(3) Rifles.

(4) Shotguns.

(5) Other instruments designed to expel a potentially lethal projectile, as designated by the commanding officer.

b. All Navy installations and activities shall implement procedures for the strict control and accountability of

personal weapons on board. Procedures shall include, but are not limited to:

(1) Registration, inventory, and deregistration of personal weapons.

(2) Identification of all personal weapons. Firearms will be identified by manufacturer, caliber, model and serial number.

(3) Semiannual sight inventories by serial number of personal weapons stored in armories or weapons containers.

(4) Storage of personal weapons.

c. Registration Requirements

(1) Weapons shall be registered within 72 hours after being introduced aboard.

(2) Weapons are not required to be brought in to be registered.

(3) Registrant must present proof of ownership.

d. Storage. Personal weapons introduced into an installation or activity will be stored in an approved armory or weapons container. Personal weapons shall not be kept or stored in barracks, bachelor officer quarters, bachelor enlisted quarters, evidence lockers (unless the weapon is controlled as actual evidence), or with security force in-service storage areas/containers.

(1) Host commands should provide storage for tenant command personal weapons, particularly those tenant commands without approved armories or available storage containers.

(2) Personnel residing in family housing may store their (registered) weapon(s) in their quarters at the discretion of the installation (host) commanding officer.

e. Lost, Sold or Stolen Personal Weapons

(1) The loss or sale of personal weapons will be promptly reported to the security officer.

(2) Discovery of stolen personal weapons will be immediately reported to the security officer.

f. Concealed Weapons. Personal weapons shall not be carried concealed aboard a Navy installation or activity.